CLAIMS

We Claim:

1. In a computer system comprising a processor and a memory, a method for detecting viruses in macros, the method comprising:

obtaining comparison data including information for detecting a virus;

retrieving a macro;

decoding the macro to produce a decoded macro; and

scanning the decoded macro for a virus by comparing the decoded macro to the comparison data.

2. The method of claim 1, further comprising:

removing the virus from the macro to produce a treated macro if the step of scanning the decoded macro indicates that the macro is infected with the virus.

3. The method of claim 1, wherein the step of retrieving a macro comprises:

accessing a targeted file;

determining whether the targeted file is a template file;

if the targeted file is not a template file, determining whether the targeted file includes an embedded macro; and

if the targeted file includes an embedded macro, locating the embedded macro.

4. The method of claim 1, wherein the comparison data includes a first suspect instruction identifier and a second suspect instruction identifier.

5. The method of claim 4, wherein the step of scanning the decoded macro to determine whether it includes a virus comprises:

determining whether the decoded macro includes a first portion which corresponds to the first suspect instruction identifier;

determining whether the decoded macro includes a second portion which corresponds to the second suspect instruction identifier; and

determining that the decoded macro includes the virus if the decoded macro includes the first and second portions.

6. The method of claim 5, wherein the first suspect instruction identifier detects a macro virus enablement instruction.

7. The method of claim 6, wherein the second suspect instruction identifier detects a macro virus reproduction instruction.

8. The method of claim 4, wherein the step of removing the virus comprises:

locating a first suspect macro instruction in the decoded macro which corresponds to the first suspect instruction identifier; and

removing the first suspect macro instruction.

9. The method of claim 8, further comprising:

verifying the integrity of the treated macro; and

replacing the infected macro in a targeted file with the ~~repaired~~ treated macro dependent upon the integrity verification of the treated macro.

10. The method of claim 8, wherein the step of removing the first suspect macro instruction includes replacing the first suspect instruction with a benign instruction.

11. The method of claim 8, wherein the step of removing the virus comprises:

locating a second suspect macro instruction in the decoded macro which corresponds to the second suspect instruction identifier; and

removing the second suspect macro instruction from the decoded macro to ~~produce a treated macro.~~

12. The method of claim 1, wherein the comparison data includes a plurality of sets of suspect instruction identifiers.

13. The method of claim 12, wherein ~~a first set of~~ suspect instruction identifiers comprises the strings ~~73~~ CB 00 0C 6C 01 00 and 67 C2 80.

14. The method of claim 13, wherein a second set of suspect instruction identifiers comprises the strings 73 CB 00 0C 6C 01 00 and 64 6F 02 67 DE 00 73 87 01 12 73 7F, a third set of suspect instruction identifiers comprises the strings 73 CB 00 0C 6C 01 00 and 6D 61 63 72 6F 73 76 08, a fourth set of suspect instruction identifiers comprises the strings 12 6C 01 00 and 64 67 C2 80 6A 0F 47, and a fifth set of suspect instruction identifiers comprises the strings 79 7C 66 6F 72 6D 61 74 20 63 6A and 80 05 6A 07 43 4F 4D.

15. In a computer system comprising a processor and a memory, a method for detecting viruses in macros, the method comprising:

retrieving a macro;

obtaining comparison data for detecting a virus, the comparison data including a first suspect instruction identifier and a second suspect instruction identifier;

scanning the macro to determine whether the macro includes a first portion which corresponds to the first suspect instruction identifier;

scanning the macro to determine whether the macro includes a second portion which corresponds to the second suspect instruction identifier; and

determining that the macro is infected with the virus if the macro includes the first and second portions.

16. The method of claim 15, further comprising:

treating the macro to produce a treated macro if it is determined that the macro includes the first and second portions.

17. The method of claim 16, wherein the step of treating the macro comprises:

locating a first macro instruction in the infected macro which corresponds to the first suspect instruction identifier; and

removing the first macro instruction from the infected macro to repair the infected macro.

18. The method of claim 17, wherein the step of treating the macro comprises:

locating a second macro instruction in the infected macro which corresponds to the second suspect instruction identifier; and

removing the second macro instruction from the infected macro to repair the infected macro.

16 12

19. The method of claim 15, wherein the step of retrieving a macro comprises:

accessing a targeted file; and

determining whether the targeted file is a template file;

if the file is not a template file, determining whether the targeted file includes an embedded macro; and

if the file includes an embedded macro, locating the embedded macro.

20. The method of claim 15, wherein the first instruction identifier includes the string 73 CB 00 0C 6C 01 00 and the second suspect instruction identifier includes the string 67 C2 80.

17 12

21. The method of claim 15, wherein the comparison data includes a plurality of sets of suspect instruction identifiers.

B6

22. The method of claim 21, wherein a first set of suspect instruction identifiers comprises the strings 73 CB 00 0C 6C 01 00 and 67 C2 80, a second set of suspect instruction comprises the strings 73 CB 00 0C 6C 01 00 and 64 6F 02 67 DE 00 73 87 01 12 73 7F, a third set of suspect instruction identifiers comprises the strings 73 CB 00 0C 6C 01 00 and 6D 61 63 72 6F 73 76 08, a fourth set of suspect instruction identifiers comprises the strings 12 6C 01 00 and 64 67 C2 80 6A 0F 47, and a fifth set of suspect instruction identifiers comprises the strings 79 7C 66 6F 72 6D 61 74 20 63 6A and 80 05 6A 07 43 4F 4D.

A 16

23. The method of claim 15, further comprising:

accessing a targeted file; and

locating the macro within the targeted file;

removing the macro from the targeted file; and

37

adding the treated macro to the targeted file to produce a corrected file.

24. An apparatus for detecting viruses in macros, the apparatus comprising:
a virus information module, for storing comparison data for detecting a virus, the comparison data including a first suspect instruction identifier and a second suspect instruction identifier; and
a macro virus scanning module, in communication with the virus information module, for receiving the comparison data and scanning a macro to determine whether the macro includes a first portion which corresponds to the first suspect instruction identifier and a second portion which corresponds to the second suspect instruction identifier.

25. The apparatus of claim 24, further comprising:
a macro locating and decoding module, in communication with the macro virus scanning module, for accessing a targeted file, determining whether the targeted file is a template file, determining whether the targeted file includes an embedded macro, and decoding the macro to produce a decoded macro.

26. The apparatus of claim 25, further comprising:
a macro treating module, in communication with the virus information module, for accessing the decoded macro and removing a first macro instruction which corresponds to the first suspect instruction identifier and a second macro instruction which corresponds to the second suspect instruction identifier to produce a treated macro.

27. The apparatus of claim 26, further comprising:

a file correcting module, in communication with the macro treating module, for accessing the targeted file, locating the macro within the targeted file, removing the macro from the targeted file and adding the treated macro to the targeted file to produce a corrected file.

28. The apparatus of claim 27, wherein the first instruction identifier includes the string 73 CB 00 0C 6C 01 00 and the second suspect instruction identifier includes the string 67 C2 80.

29. The apparatus of claim 27, wherein the comparison data includes a plurality of sets of suspect instruction identifiers.

30. The apparatus of claim 29, wherein a first set of suspect instruction identifiers comprises the strings 73 CB 00 0C 6C 01 00 and 67 C2 80, a second set of suspect instruction comprises the strings 73 CB 00 0C 6C 01 00 and 64 6F 02 67 DE 00 73 87 01 12 73 7F, a third set of suspect instruction identifiers comprises the strings 73 CB 00 0C 6C 01 00 and 6D 61 63 72 6F 73 76 08, a fourth set of suspect instruction identifiers comprises the strings 12 6C 01 00 and 64 67 C2 80 6A 0F 47, and a fifth set of suspect instruction identifiers comprises the strings 79 7C 66 6F 72 6D 61 74 20 63 6A and 80 05 6A 07 43 4F 4D.

31. An apparatus for detecting viruses in macros, the apparatus comprising:

means for obtaining comparison data for detecting a virus, the comparison data including a first suspect instruction identifier and a second suspect instruction identifier;

means for scanning the macro to determine whether a macro includes a first portion which corresponds to the first suspect instruction identifier;

means for scanning the macro to determine whether the macro includes a second portion which corresponds to the second suspect instruction identifier; and

means for determining that the macro is infected with the virus if the macro ~~includes the first and second portions.~~

25 24

32. The apparatus of claim ~~31~~, further comprising:

means for locating a first macro instruction and a second macro instruction within the macro which respectively correspond to the first suspect instruction identifier and the second suspect instruction identifier; and

means for removing the first macro instruction and the second macro instruction from the macro to produce a treated macro.

33. The apparatus of claim 32, further comprising:

means for accessing a targeted file and determining whether the targeted file includes a macro.

34. The apparatus of claim 33, further comprising:

means for correcting a file, the means for correcting a file including means for accessing the targeted file, means for removing the macro from the targeted file and means for adding the treated macro to the targeted file to produce a corrected file.

35. A system for detecting viruses in macros, the system comprising:

34

a memory, for storing routines and comparison data for detecting a virus, the comparison including a first suspect instruction identifier and a second suspect instruction identifier; and

a processor, in communication with the memory, for receiving the comparison data and scanning a macro to determine whether the macro includes a first portion which corresponds to the first suspect instruction identifier and a second portion which corresponds to the second suspect instruction identifier.